

Arithmétique, dénombrement et probabilités finies

Trois domaines discrets qui se répondent : les **congruences**, les **coefficients binomiaux** et les **lois usuelles**.

Arithmétique

Théorème — Bézout et Gauss

$a \wedge b = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}, au + bv = 1$. **Gauss** : si $a|bc$ et $a \wedge b = 1$, alors $a|c$. Si $a|c$, $b|c$ et $a \wedge b = 1$, alors $ab|c$. Algorithme d'Euclide étendu pour trouver u, v .

Théorème — nombres premiers, Fermat

Décomposition unique en facteurs premiers ; infinité des nombres premiers. **Petit théorème de Fermat** : pour p premier et $a \wedge p = 1$, $a^{p-1} \equiv 1 [p]$; pour tout a , $a^p \equiv a [p]$. Les congruences sont compatibles avec $+$ et $\times$.

Dénombrement

Propriété — cardinaux

$|A \cup B| = |A| + |B| - |A \cap B|$; $|A \times B| = |A| |B|$; $|\mathcal{P}(E)| = 2^n$; nombre d'applications de E (p éléments) dans F (n) : n^p ; d'injections : $\frac{n!}{(n-p)!}$; de bijections de E : $n!$; de parties à p éléments : $\binom{n}{p}$. Binôme : $(a+b)^n = \sum_k \binom{n}{k} a^k b^{n-k}$; formule de Vandermonde $\sum_k \binom{n}{k} \binom{m}{n-k} = \binom{m+n}{n}$.

Probabilités finies

Théorème — Bayes et probabilités totales

Pour un système complet (A_i) : $P(B) = \sum P(A_i) P_{A_i}(B)$ et

$$P_B(A_i) = \frac{P(A_i) P_{A_i}(B)}{\sum_j P(A_j) P_{A_j}(B)}.$$

Formule des probabilités composées :

$$P(A_1 \cap \dots \cap A_n) = P(A_1) P_{A_1}(A_2) \dots P_{A_1 \cap \dots \cap A_{n-1}}(A_n).$$

Définition — indépendance

A, B indépendants si $P(A \cap B) = P(A)P(B)$. Indépendance **mutuelle** d'une famille : pour toute sous-famille, la probabilité de l'intersection est le produit (plus fort que l'indépendance deux à deux).

Définition — variables aléatoires, lois usuelles

Loi $P(X = x)$, loi conjointe $P(X = x, Y = y)$, lois marginales. Uniforme sur $\{1, \dots, n\}$: $E = \frac{n+1}{2}$. Bernoulli $\mathcal{B}(p)$: $E = p$, $V = p(1-p)$. Binomiale $\mathcal{B}(n, p)$: $E = np$, $V = np(1-p)$.

Propriété — espérance, variance, covariance

$E(X) = \sum x P(X = x)$, linéaire ; formule de transfert $E(g(X)) = \sum g(x) P(X = x)$.
 $V(X) = E(X^2) - E(X)^2$, $V(aX + b) = a^2 V(X)$.
 $\text{Cov}(X, Y) = E(XY) - E(X)E(Y)$; $V(X + Y) = V(X) + V(Y) + 2\text{Cov}(X, Y)$. X, Y indépendantes $\Rightarrow E(XY) = E(X)E(Y)$ et $\text{Cov} = 0$ (réciproque fausse).
 Inégalités de Markov et de Bienaymé-Tchebychev.

Questions fréquentes sur ce chapitre

Que dit le théorème de Gauss ?

Si a divise bc et a est premier avec b , alors a divise c .

Quel est le petit théorème de Fermat ?

Pour p premier et a non divisible par p , $a^{p-1} \equiv 1 \pmod{p}$.

Comment calculer le nombre d'injections de E dans F ?

Si $|E| = p$ et $|F| = n$ avec $p \leq n$: $\frac{n!}{(n-p)!}$.

Quelle est la formule de Bayes ?

$P_B(A) = \frac{P(A)P_A(B)}{P(B)}$, avec $P(B)$ calculée par la formule des probabilités totales.